

Washington Public Ports Association
P.O. Box 1518
Olympia, WA 98507-1518

Docket Management Facility (USCG-2003-14733)
U.S. Department of Transportation
Room PL-401
400 Seventh St. S.W.
Washington, D.C. 20590-0001

July 31, 2003

Thank you for the opportunity for the Washington Public Ports Association to comment on the U.S. Coast Guard's Interim Final Regulations on Maritime Security. First, the WPPA supports the position on the rules represented by the American Association of Port Authorities. In addition, WPPA would like to amplify the comments on selected points that are particularly relevant to the Washington state port system.

By way of background, please be aware there are 76 public port districts in Washington state. The ports are involved in activities ranging from marina operations, to airports, industrial development and marine terminals. WPPA's view is that there are 16 ports that may be subject to the proposed regulations. These ports are located on Puget Sound, Grays Harbor on the Washington coast and along the Columbia/Snake River system.

They vary greatly in size and in the volumes and types of cargo (i.e. containers, bulk, break-bulk, neo-bulk) that they handle. They also vary greatly in terms of the risks their operations pose and significantly in the amount of revenues they generate.

The risk versus revenues relationship is particularly relevant for purposes of these comments. Some of our ports provide vital transportation services to their communities but operate on very thin margins. Significant new costs associated with complying with the proposed regulations could threaten the continued viability of some of our smaller ports.

Also, WPPA would like to note that some of our ports operate their own marine terminal facilities while others lease operations to private sector terminal operators. Any new rule should allow for diverse approaches to security management that include different types of public port districts.

With that as background, please consider the following comments especially in connection with smaller, low-risk ports:

1. The regulations need to provide more clear guidance regarding which are required to develop security plans.
2. Improved technical assistance must be provided to help such ports determine if they are required to develop plans, particularly as it relates to 33 CFR Part 105.105. Additional assistance also is necessary - once a go-ahead decision has been made - to develop adequate security plans.

3. Funding assistance will be necessary to develop and especially to implement security plans.

Please note that also attached are comments from the Port of Pasco with which the WPPA concurs. The comments relate to 33 CFR Parts 101, 102, 103, et al., and 46 CFR Parts 2, 31, 71, et al. Also attached is the comment letter from AAPA.

Port officials in Washington state recognize the difficulty of developing a plan that provides adequate security for our nation's port system and remain committed to assuming their fair share of the burden for this effort.

Sincerely,

Scott Taylor, Assistant Director
Washington Public Ports Association

Comments to 33 CFR Parts 101,102,103, et al. and
46 CFR Parts 2,31,71, et al.
by the Port of Pasco
July 29, 2003

General Comments:

1) Will these CFR's change the existing guidance in the NVIC 11-02 prior to being issued for implementation (as opposed to guidance)?
The rules require that Facility Security Plans be submitted to COTP by 12/29/03, with implementation in place by 6/30/04.

Specific Comments:

33CFR Part 103, Area Maritime Security

2) Page 39291, Subpart C- Area Maritime Security (AMS) Committee. Need clarification on this. Does the rule describe the AMS Committee for all the affected Ports or is this a central committee under the COTP?? Further, if this describes the committees for all ports, then the membership (section 103.305) appears too restrictive. Paragraph [a] states " An AMS Committee must be composed of not less than seven members, each having at least 5 years of experience related to maritime or port security operations...." This could be difficult to achieve. Suggest providing words that say "recommend maritime experienced members" .

33CFR Part 105, Facility Security

3) Page 39325, section 105.220 "Drill and exercise requirements", paragraph [b] states that the FSO must ensure that at least one security drill is conducted every 3 months. Suggest conducting drill every 6 months.

4) Page 39329, section 105.275, "Security Measures for Monitoring", paragraph [a], discusses security measures to be implemented using various intrusion devices, security guards, etc.. Suggest adding existing staff/employees as

another measure in detecting suspicious activities to this paragraph. Smaller ports will rely upon existing staff/employees along with other measures implemented.

Before the
U.S. COAST GUARD
Washington, D.C.

July 31, 2003

Request for Comments on
Coast Guard Interim Final Regulations
On Maritime Security
33 CFR Parts 101 and 102

USCG-2003-14792

Comments of the

AMERICAN ASSOCIATION OF PORT AUTHORITIES
1010 Duke Street  Alexandria, VA 22314  (703) 684-5700

AMERICAN ASSOCIATION OF PORT AUTHORITIES
Comments on
Coast Guard Interim Final Regulations
on Maritime Security
- July 31, 2003 -

Founded in 1912, the American Association of Port Authorities (AAPA) represents almost 150 public ports in Canada, the Caribbean, Latin America, and the United States. In addition, the Association represents almost 300 sustaining members - firms and individuals with an interest in the seaports of the Americas.

This response is filed on behalf of AAPA's U.S. delegation. U.S. ports serve vital national interests by facilitating the flow of trade and cruise passengers and supporting the mobilization and deployment of U.S. troops. In the next twenty years, U.S. overseas international trade, 95% of which enters or exits through the nation's ports, is expected to double. As the link between the land and the water, ports continue to update and modernize their facilities not only to accommodate this growth, but also to ensure homeland security.

We cannot stress enough that final maritime security regulations must be sensitive to the unique nature and complexity of America's port industry, which is vast, diverse and highly competitive. Our U.S. member ports range from huge

load centers handling millions of tons of containerized, breakbulk, dry and liquid bulk cargos, to relatively small "niche" ports serving the needs of a particular region. Not all ports will need the same level of security depending on their location, level of risk and the type of commodities. For example, small ports or facilities that handle low-risk, low-value commodities (i.e., dry bulk cargo) are very price sensitive and are at risk of being put out of business if they were to fully implement the regulations in 33 CFR Part 105. Each facility must have the flexibility to develop security programs that address its unique security issues in a cost-effective manner.

While individual facility security plans will vary, there must be some consistency in the way plans are reviewed. Guidance should be issued to the Captains of the Port so that a consistent approach is used. Further, with regard to low-risk small ports, the USCG must be open to approving alternative plans that are not as costly as those outlined in the regulations.

Ports also differ in the way they are operated. Port authorities are state and local government entities that oversee the management of public ports. There are operating, landlord and limited operating ports. Operating ports are those in which cargo handling inland from the pier is performed by port authority employees. At landlord ports, these functions are performed by tenants, such as terminal operators, who lease property from the port. Limited operating ports combine these roles, leasing some facilities and operating others. With such varied control over port operations and facilities, what works in one port to address security may not work in another port. Furthermore, security programs at ports vary and are tailored to the unique environment of each port.

Federal help is essential to ensure that these maritime security regulations can be implemented quickly to protect Americans from acts of terrorism. Without more Federal help, costs to implement mandated security enhancements will severely impact public ports' ability to invest in required infrastructure improvements such as facility expansion, efficiency improvements, channel deepening projects, and navigational aids to meet the growth in trade. The long-term impact will be significant and will be detrimental to the ability of ports to handle the projected growth in maritime trade. By inadequately funding security mandates, the nation likely will face a lack of capacity or see growing inefficiencies in the system in the future. If costs to port facilities increase significantly, diversion of cargo to ports in Canada and Mexico will occur, and U.S. exports, which are primarily low-value, will become non-competitive.

COMMENTS ON INTERIM FINAL FACILITY REGULATIONS (33 CFR Part 105)

Part 105.105 - Applicability

A number of port facilities are covered under Part 105 that handle low value/low risk non-hazardous commodities (such as dry bulk commodities including stone, iron ore, urea, grain, salt and cement). These types of commodities are extremely price sensitive and vulnerable to factors such as security demands that can increase operating costs. Though the Coast Guard provides waiver and alternative programs in the regulations, we believe that there must be more flexibility for these low-risk facilities. The Association seeks a modification to the regulations that would provide more flexibility to these facilities earlier in the process to develop an approach that is risk-based and cost-

effective. There is strong concern that the costs of implementing the process prescribed in the Interim Regulations simply to reach the potential waiver/alternative program phase will be significant enough to make many commodities non-competitive and/or result in facility closures.

Low-risk port facilities will not need the same level of security as other facilities that are at a higher risk of a security incident. This is not adequately addressed in the regulations. Some of these facilities also handle price-sensitive commodities, and we urge the Coast Guard to carefully consider the impact of security regulations on these facilities. For example, the first year costs to implement the facility security regulations at an iron ore facility would be a \$1.50 per ton increase for infrastructure improvements and an additional 10 cents a ton to conduct a Facility Security Assessment and to pay for a Facility Security Officer. An example is Brazilian ore that is delivered to the lower Great Lakes mills through the river system – it is highly competitive. The cost of security could drive an iron ore facility out of business. Another example is grain. The differential for imported versus exported grain trades is as low as ¼ cent per bushel, so a half cent per bushel increase can shift grain trade dramatically. Increases in security costs for these facilities could make U.S. grain less competitive with other countries.

There currently is no Federal help available for these facilities. Because they are considered low risk, they are not rated high enough to qualify for the Transportation Security Administration's (TSA) Port Security Grant Program. The TSA program can offer facilities less than 10% of the funds needed to make facility enhancements, so most funds go to high-risk ports.

Also under applicability, we request that the Coast Guard list the references of those covered by the regulations instead of including a cascading list of references to the CFR.

Part 105.115 - Compliance

According to the regulations, a facility must implement its plan by July 1, 2004. Does this mean that everything that is outlined in the plan must be in place and operational, or does it mean that the facility has implemented the plan? If full compliance is required by next July, this raises a number of serious concerns such as adequate funding and timing for hiring suitable contractors and vendors. Ports and facilities will not have the money or be able to obtain contracts to be in full compliance with the plan by July 2004.

Part 105.200 - Owner or Operator

AAPA seeks clarification of the definition of owner or operator and requests that the definition be listed under Part 105.200. The Coast Guard defines owner or operator as "any person or entity that maintains operational control over any facility, vessel, or OSC facility subject to the requirements of this subchapter." AAPA requests that operational control be further defined in the definition of owner or operator. AAPA offers the following definitions for your consideration and encourage that they be adopted in the final rule: "operational control is the ability to influence or control the physical or commercial activities pertaining to that facility for any period of time."

Part 105.205 - Facility Security Officer (FSO)

AAPA believes that the requirements for the Facility Security Officer (FSO) are excessive and unattainable. The industry is concerned that there are very few security professionals who could meet these qualifications. If the FSO is

required to have the level of expertise identified in the regulations, then the USCG must provide training for these individuals.

Part 105.230 - Maritime Security (MARSEC) Level Coordination and Implementation Under Part 105.230 (b)(1), AAPA asks the Coast Guard to delete "and vessels scheduled to arrive at the facility within 96 hours." AAPA believes that the USCG should be responsible to maintain radio contact with vessels due to arrive at the port and can do this easily with a broadcast notice to mariners. Then the Coast Guard should notify the facility so plans can be made to exchange the DOS (see additional comments on the DOS below). The facility operator should not be in the middle of communicating this information back and forth with the Coast Guard and the vessel because it will cause too much confusion and will not be efficient. The facility operator will maintain contact with vessels moored to the facility.

Also, under 105.230 (e), we ask that the Coast Guard strike "which may include but are not limited to:

- (1) Use of waterborne security patrol;
- (2) Use of armed security personnel to control access to the facility and to control access to the facility and to deter, to the maximum extent practical, a transportation security incident; and
- (3) Examination of piers, wharves, and similar structures at the facility for the presence of dangerous substances or devices underwater or other threats."

We believe that use of waterborne security patrols is inappropriate because facility operators do not have jurisdictional control or authority over the Federal channel. With regard to armed security personnel (2), this must be determined on a case-by-case basis and coordinated with local law enforcement. Finally, examination of piers, wharves and similar structures is difficult because resources are limited and many facilities do not have the capability to do this.

Part 105.245 - Declaration of Security

AAPA believes that facilities must have the ability to exchange the Declaration of Security (DOS) electronically. The exchange of a DOS in paper form is inefficient, could cause delays for certain operations, and would require significant personnel resources.

Part 105.255 - Security Measures for Access Control

Because the Transportation Worker Identification Card (TWIC) will not be fully operational for several years, ports and facilities will have to address access control on an individual basis. According to the regulations, the Department of Homeland Security will be issuing interim guidance on access control. The port industry believes that this guidance should be issued quickly and it should provide clear direction on who should be denied access to the facility. The guidance must address the issue of background checks and outline who will handle this, who pays for it, and what agencies will be involved. The guidance on background checks must be based on the Maritime Transportation Security Act.

Many ports have already begun to implement their own credentialing systems with varying technologies and complexity. It will be very costly for these ports to comply with a new credentialing program. Though guidance is necessary in the short term, AAPA strongly urges the Transportation Security Administration to implement a national TWIC program as soon as possible.

Part 105.265 - Security Measures for Handling Cargo

The Coast Guard should make exceptions for a facility that handles undocumented or unassigned cargo. To address this we recommend changing Part 105.265 (a) (6) to read "restrict the entry of unidentified cargo to the facility that does not have a confirmed date for loading, as appropriate." We would also like clarification on what the Coast Guard means by "restrict."

This change is important because a number of our member ports warehouse cargo for customers. For example, one of AAPA's member ports stores wood pulp and other commodities for its customers that for various reasons do not ship their cargos upon delivery to the port and rent space from the port authority to warehouse the goods.

Part 105.275 - Security Measures for Monitoring

AAPA asks the Coast Guard to strike the words "waterborne patrols" in Part 105.275 (a) and (c) (2). Again, the port or facility does not have jurisdiction over the Federal channel.

Also, in Part 105.275 (a) strike the word "continuously" and define monitor as a "systematic process for providing surveillance for a facility."

Part 105.410 - Submission and Approval

The local Captain of the Port (COTP) is charged with reviewing Facility Security Plans, but it is unclear what criteria will be used and if these will vary within each port district. Procedures must be developed for how the COTP approves plans. The Coast Guard must approach the appropriate industry groups and work with them to come up with best practices that can be used in developing and approving plans. This must be done as quickly as possible. Also, it would be helpful for the Coast Guard to identify several standardized methodologies for conducting risk assessments.

Part 105.415 - Amendment and Audit

We recommend that the Coast Guard modify Part 105.415 (4) (ii) to read "not have regularly assigned duties for that facility." This would allow flexibility for audits to be conducted by individuals with security-related duties as long as those duties are not at that facility.

AREA MARITIME SECURITY

Part 103.300 - Area Maritime Security Committee

Part 103.300 (b) (6) says that the charter for the Security Committee should address the rules for handling and protecting classified, security sensitive, commercially sensitive, and proprietary information. AAPA believes that there is not enough information available defining security sensitive information. We ask that the Coast Guard provide immediate uniform guidance on the handling of security sensitive information. This should not be left up to the Security Committee to handle.

In comments submitted to the Coast Guard on February 25, 2003, AAPA states "there must be a way of protecting security sensitive information. An SSI

classification is appropriate. However, the Coast Guard must provide training/information to ports on how to classify documents as SSI. One problem that ports have run into in the past is that some state laws require full disclosure of public documents, which includes security plans and things that should not be available to the public. The Federal government must preempt state laws when it comes to SSI or develop a mechanism that ports can follow to protect their secure documents."

AMERICAN ASSOCIATION OF PORT AUTHORITIES

1010 Duke Street - Alexandria, VA 22314 - (703) 684-5700